Abstract

English

This 92-page thesis (featuring 9 tables, 32 figures, and 85 references) presents the development of an innovative browser extension for comprehensive phishing attack prevention. Research relevance is driven by the exponential surge in phishing incidents (>1.2 million documented cases in 2023) and critical limitations of rule-based defense systems. The primary objective is to engineer a high-precision real-time detection tool minimizing user experience disruption. Methodology integrates:

- **Machine learning:** Random Forest ensemble trained on 6.5 million URLs — achieving 96.2% precision and 93.7% recall;
- **Deep DOM analysis:** for identifying cloned authentication interfaces, hidden elements, and visual mimicry;
- **API integration:** with Google Safe Browsing and VirusTotal for global threat intelligence verification;
- **Modular architecture:** client–server setup with Chrome Extension and Flask backend.

Experimental results show: ROC-AUC 0.983, false positive rate <0.1%, response latency <250 ms. User testing (30 participants) validated interface efficacy (average usability score: 9.2/10). The study contributes to client-side cybersecurity theory and delivers a production-ready solution for enterprise deployment.

Русский

Настоящая дипломная работа объёмом 92 страницы (включая 9 таблиц, 32 рисунка и 85 библиографических источников) посвящена разработке инновационного браузерного расширения для комплексного предотвращения фишинговых атак. Актуальность исследования обусловлена экспоненциальным ростом фишинговых инцидентов (свыше 1.2 млн подтверждённых случаев в 2023 г.) и принципиальными ограничениями традиционных методов защиты, основанных на статических правилах. Цель работы — создание высокоточного инструмента для детектирования фишинга в режиме реального времени с минимальным воздействием на пользовательский опыт. Методология включает:

- **Машинное обучение:** ансамбль Random Forest, обученный на 6,5 миллионах URL — достигший 96,2% точности и 93,7% полноты;

- **Глубинный анализ DOM:** для выявления клонированных интерфейсов аутентификации, скрытых элементов и визуального мошенничества;
- **Интеграция API:** с Google Safe Browsing и VirusTotal для проверки через глобальные базы угроз;
- **Модульная архитектура:** клиент–сервер с расширением Chrome и бэкендом Flask.

Результаты тестирования демонстрируют: ROC-AUC 0.983, ложные срабатывания <0.1%, задержка ответа <250 мс. Пилотное внедрение с участием 30 пользователей подтвердило эффективность интерфейса (средняя оценка юзабилити — 9.2/10). Работа вносит вклад в теорию клиентской кибербезопасности и предоставляет готовое решение для интеграции в корпоративные среды.

Қазақша

Бұл 92 беттен тұратын дипломдық жоба (оған 9 кесте, 32 сурет және 85 әдеби көздер кіреді) фишингке қарсы кешенді қорғаныс жүйесін құруға арналған браузер кеңейтімін әзірлеуге арналған. Зерттеу өзектілігі – 2023 жылы 1,2 млн-нан астам расталған фишинг оқиғаларының экспоненциалды өсуі және статикалық ережелерге сүйенетін дәстүрлі қорғаныс әдістерінің шектеулілігімен түсіндіріледі. Жұмыстың мақсаты – пайдаланушы тәжірибесіне минималды әсер ете отырып, фишингті нақты уақыт режимінде жоғары дәлдікпен анықтайтын құралды жасау. Методологияға мыналар кіреді:

- **Машиналық оқыту:** 6.5 миллион URL-қа негізделген ансамбльдік алгоритм Random Forest — дәлдігі 96,2% және толықтығы 93,7%;
- **DOM терең талдауы:** жалған аутентификация интерфейстерін, жасырын элементтер мен визуалды алаяқтықты анықтау үшін;
- **API-интеграциясы:** Google Safe Browsing және VirusTotal арқылы жаһандық қауіп-қатерлер базасымен бірлесе жұмыс істеу;
- **Клиент–сервер архитектурасы:** модульдік, Chrome кеңейтімі мен Flask-бэкенд.

Тестілеу нәтижелері: ROC-AUC — 0,983, жалған позитивтер <0,1%, жауап беру уақыты <250 мс. 30 пайдаланушы қатысқан пилоттық енгізуде интерфейстің тиімділігі расталды (пайдаланушылық бағалау орташа бағасы – 9,2/10). Жоба клиенттік киберқауіпсіздік теориясына үлес қосып, корпоративті ортаға ендіруге дайын шешімді ұсынады.